Department of Defense

FACT SHEET: Defense Industrial Base (DIB) Cybersecurity Activities
May 11, 2012

The United States continues to face a significant risk that critical Defense information residing on DIB networks and systems can be compromised by malicious cyber actors resulting in potential economic losses or damage to United States national security. The Department of Defense is actively engaged in multiple efforts to foster mutually beneficial partnerships with the Defense Industrial Base (DIB) to protect Department of Defense information residing on or passing though DIB systems. One such effort is the DIB Cyber Security/Information Assurance (CS/IA) Program, including its optional Enhanced Cybersecurity Services (ECS) component.

Bilateral Information Sharing

The DIB CS/IA Program is designed to improve DIB network defenses and allows DIB companies and the Government to reduce damage to critical programs when defense information is compromised. The DIB CS/IA Program includes a voluntary information sharing component under which DIB companies and the Government agree to share cyber security information out of a mutual concern for the protection of sensitive but unclassified information related to DoD programs on DIB company networks.

Under the DIB CS/IA Program, DoD provides participating DIB Companies with unclassified indicators and related, classified contextual information. DIB companies can choose whether to incorporate the indicators into their own traffic screening or other security tools, and they can review or act on the contextual information as they wish to better address the cybersecurity threats they face. DoD also shares mitigation measures to assist DIB Companies' cybersecurity efforts.

DIB companies also report known intrusion events to the Government and may participate in Government damage assessments, if needed. A DIB company may report any cybersecurity event that may be of interest to the cyber community, at its discretion.

DIB Enhanced Cybersecurity Services (DECS)

As an additional and optional part of the program, the Government will furnish classified threat and technical information to voluntarily participating DIB Companies or their Commercial Service Providers (CSPs). This sensitive Government furnished information enables the DIB companies, or the CSPs on behalf of their DIB customers, to counter additional types of known malicious activity and to further protect Department of Defense program information.

Any CSPs that are capable of implementing the Government furnished information in compliance with security requirements are eligible to participate and offer the cybersecurity services to participating DIB companies. CSPs may also charge for providing this service to participating DIB companies.

The DECS is a joint activity with the Department of Homeland Security (DHS), falling under the umbrella of DHS' Joint Cybersecurity Services Program, part of the DHS-led effort to protect U.S. critical infrastructure. DHS is the government point of contact for CSPs under the JCSP and DECS.

DIB Company Participation

To participate in the DIB CS/IA Program, eligible DIB companies sign a Framework Agreement with DoD. Once in the DIB CS/IA Program, a DIB company may also elect to participate in the ECS component in several different ways: by meeting the security requirements to implement the countermeasures on its own networks, by

purchasing the services from a participating CSP, or by meeting the requirements to become a CSP to offer the services to other DIB companies.

The DIB CS/IA Program is open to all eligible DIB companies. The content, manner, and means by which DIB companies participate are captured in a Framework Agreement between DoD and the DIB company. More information, including eligibility requirements, is available in the Federal Register at http://www.gpo.gov/fdsys/pkg/FR-2012-05-11/pdf/2012-10651.pdf, and on the DIB CS/IA Program public website (http://dibnet.dod.mil/).